

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARYBefore the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Communications Assistance for Law
Enforcement Act

))))
CC Docket No. 97-213COMMENTS OF
THE PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION

Eric W. DeSilva
Stephen J. Rosen
Daniel J. Smith
WILEY, REIN & FIELDING
1776 K Street, N.W.
Washington, DC 20006-2304
(202) 429-7000

Its Attorneys

December 14, 1998

Mary McDermott
Senior Vice President/Chief of Staff for
Government Relations
Todd B. Lantor
Manager, Government Relations
PERSONAL COMMUNICATIONS
INDUSTRY ASSOCIATION
500 Montgomery Street, Suite 700
Alexandria, VA 22314
(703) 739-0300

No. of Copies rec'd 074
List A B C D E

SUMMARY

The Communications Assistance for Law Enforcement Act (“CALEA” or the “Act”) represents a legislative compromise between the needs of law enforcement, the progress of the communications industry, and the privacy of Americans. In striking this balance Congress made a choice that CALEA would be interpreted narrowly, would safeguard the privacy of communications not authorized to be intercepted, and would not provide law enforcement officials with capabilities beyond what they enjoy today. It is crucial that the Commission not disrupt this delicate balance by expanding the scope of the assistance capability requirements beyond the narrow requirements Congress set forth in CALEA. The Commission can do so by implementing J-STD-025, the industry’s CALEA standard for two-way voice telephony, as it is written.

In this proceeding, the Commission has correctly identified the three critical components of the Act that will guide its analysis of each assistance capability, or punch list item, requested by the FBI. First, the FCC must determine whether the information is “call-identifying information.” In so doing, the Commission should be aware that Congress views “call identifying information” as the information used to route a call, or, more specifically, the telephone numbers dialed by the subject of a warrant from his or her telephone and the telephone number associated with a call coming into the telephone of the subject of a warrant.

Second, the Commission must find that the capability is “reasonably available” to the carrier—an analysis that includes an important cost component. In order to meaningfully evaluate the cost of each punch list item, however, the Commission must, either in this proceeding or in a later proceeding, elicit the necessary cost data from industry, and put that data out for public comment. The Commission must further be aware that compliance costs will be

increased because the telecommunications industry is currently expending information technology resources grappling with the Y2K problem, and CALEA upgrades will be added to switches outside of the normal upgrade cycle. Changing capacity requirements might also have an effect on compliance costs.

Third, the agency must ensure that the four factors in Section 107(b)—cost-effective implementation, protection of customer privacy, minimizing the cost to ratepayers, and encouraging the provision of new technologies and services—are satisfied. At each step, the Commission must be guided by the intent of Congress that the capability requirements be narrowly interpreted and that the *status quo* of surveillance capabilities neither be diminished nor expanded. Therefore, if it is unclear whether an assistance capability should be included in the standard, the Commission must opt against including the requirement.

There are two punch list items that are not required by CALEA despite their inclusion in J-STD-025. These capabilities represent a compromise with law enforcement, not compliance with the statute. The first is the provision of geographic location information of a subject's mobile phone. This information is not call-identifying information, but rather, geographic-identifying information. Further, such a requirement impermissibly expands the surveillance capabilities of law enforcement beyond the *status quo*. If this requirement does remain, carriers should be permitted to satisfy it with information obtained in the ordinary course of business or pursuant to other regulatory requirements, such as E-911.

Second, carriers cannot be required to indiscriminately provide packet data to law enforcement regardless of the information within those packets. In particular, in the case of trap and trace warrants and pen registers, CALEA mandates that carriers separate out content from call-identifying information before providing this information to law enforcement officials.

Given this fact, the Commission is required under Section 107 to consider what impact the necessity of separation will have on the deployment of new technologies *before* it requires carriers to obtain and provide this information.

The Commission faithfully holds to the intent of Congress in examining three of the items law enforcement sought to add to J-STD-025. The agency's rejection of surveillance status information, continuity tone requirements, and real time feature status messages represents the correct implementation of CALEA. In each case, the Commission correctly interpreted the relevant terms narrowly and acted to ensure that the capabilities of law enforcement did not expand beyond what they enjoy today.

However, the Commission's initial conclusions regarding several other items, specifically, the provision of the content of conference calls, party status on conference calls, subject-initiated signaling, certain network signaling, timing of call information, and post cut-through dialing, do not comport with CALEA. In each case, the Commission either fails to narrowly interpret the term "call-identifying information" in the manner Congress intended, expands law enforcement's capabilities beyond the *status quo*, or neglects to consider the fact that the information sought is not "reasonably available." These capabilities must be rejected to preserve the balance Congress struck.

Providing law enforcement with call content information after a subject has dropped off of the call violates the privacy of all others on that call. Further, the Commission's interpretation of what constitutes a subscriber's facilities would open the entire to surveillance anytime the subject made a call. Party status messages for multi-party calls are not call-identifying information, as this information is not used to route calls on the network. Similarly, subject-initiated signaling information, which is analogous to party status messages (hold, transfer, flash)

in the conference call context, is not call-identifying information. Network signaling also is not call-identifying information because it too is not used to route calls. Rather, this information simply provides information about the *status* of a call, and does not identify it. The timing requirements requested by law enforcement find no support in the statute, would expand law enforcement's capabilities beyond the *status quo* and are not reasonably available. Finally, post-cut-through dialing information is really content information, not call-identifying information to the subscriber's carrier. Further such information, because it is carried on the call content channel, is not reasonably available to the subscriber's carrier.

If, despite the advice of the telecommunications industry to leave J-STD-025 intact, the Commission chooses to add any of the punch list items, the Commission should remand any standards-setting work necessitated by adding these items to TIA. In addition, the Commission must provide TIA with a reasonable amount of time to draft any new standards, and the telecommunications industry with a reasonable amount of time to manufacture, test, and deploy any equipment built to meet these standards.

Finally, the Commission should closely monitor industry efforts to set future CALEA capability requirements for those other carriers not covered by J-STD-025 such as paging, SMR and mobile satellite services. Technological differences between services, and the text of CALEA, however, limit the Commission's decisions in this proceeding specifically to the wireline, cellular and broadband PCS carriers expressly included in J-STD-025. In the case of CALEA, one size does not fit all. For example, messaging providers, who have already adopted standards for traditional and advanced paging services, are technically incapable of providing law enforcement officials with location data, and are under no regulatory obligation to gather this

information for other services. Similarly, while cloning is a sensible solution in the context of traditional messaging, it is inapplicable to two-way wireless telephony.

J-STD-025 is a delicate compromise between the needs of law enforcement, the capabilities of the telecommunications network, and costs. Therefore, PCIA respectfully requests the Commission to adopt J-STD-025 in its present form without the added "punch list" items.

CONTENTS

I. INTRODUCTION	2
II. THE ASSISTANCE CAPABILITY REQUIREMENTS ARE TO BE INTERPRETED NARROWLY AND IN A MANNER THAT PROTECTS THE PRIVACY OF THE AMERICAN PUBLIC	5
III. THREE CRITICAL COMPONENTS OF THE ACT MUST GUIDE THE COMMISSION'S ANALYTICAL APPROACH TO EACH FEATURE OF THE PUNCHLIST	7
A. Call Identifying Information	8
B. "Reasonably Available" Includes an Element of Cost Determination.....	9
C. The Section 107(b) Factors Must Be Satisfied.....	13
IV. PARTICULAR CAPABILITIES OF J-STD-025 REPRESENT INDUSTRY COMPROMISE, NOT STATUTORY REQUIREMENTS	15
A. Geographic Location Information Is Not Required Under CALEA, Thus Information Derived In Other Contexts Can Be Used To Satisfy Law Enforcement's Requests.....	15
B. Call Content and Call Identifying Information Must Be Narrowly and Specifically Defined In the Packet Data Context.....	17
V. THE FCC'S APPROACH TO SURVEILLANCE STATUS, CONTINUITY CHECK TONE, AND FEATURE STATUS CORRECTLY COMPORTS WITH THE STATUTORY LANGUAGE AND INTENT OF CONGRESS	18
A. The Commission Correctly Interpreted CALEA To Find That Automated Delivery of Surveillance Status Information Is Not Required.....	18
B. The Commission's Conclusion Regarding the Check Tone Correctly Applies the Section 103 Factors	20
C. The Commission's Conclusion Regarding the Provision of Feature Status Further Advances the Intent of Congress.....	21
VI. THE FCC'S APPROACH TO THE REMAINING "PUNCH LIST" ITEMS IS INCONSISTENT WITH THE STATUTORY LANGUAGE AND INTENT	

OF CONGRESS	22
A. The Content of Conference Calls Can Only Be Provided When the Subject Remains Part of the Call.	22
B. Party Hold, Party Join, Party Drop Messages For Multi-Party Calls Are Not “Call Identifying Information”	25
C. Subject-Initiated Signaling Information Does Not Fall Under CALEA’s Requirements	27
D. Network-Generated In-Band and Out-of-Band Signaling	28
E. Timing of Call Identifying Information	30
F. Post-Cut-Through Dialing Information Delivered Over The Call Data Channel	32
VII. THE COMMISSION SHOULD CONTINUE ITS EXISTING ROLE IN ASSISTING THE INDUSTRY IN SETTING FUTURE CALEA CAPABILITY STANDARDS, BUT SHOULD NOT IMPOSE J-STD-025 BEYOND THE WIRELINE AND BROADBAND CMRS INDUSTRIES	34
VIII. CONCLUSION	38

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

Communications Assistance for Law
Enforcement Act

)
) CC Docket No. 97-213
)
)

**COMMENTS OF
THE PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION**

The Personal Communications Industry Association ("PCIA"),¹ by its attorneys, hereby respectfully submits its comments to the Commission's Further Notice of Proposed Rulemaking in the above-captioned proceeding.² In implementing the Communications Assistance for Law Enforcement Act ("CALEA" or the "Act"),³ the Commission must not expand the scope of the

¹ PCIA is an international trade association established to represent the interests of both the commercial and private mobile radio service communications industries and the fixed broadband wireless industry. PCIA's Federation of Councils includes: the Paging and Messaging Alliance, the Broadband PCS Alliance, the Site Owners and Managers Association, the Association of Wireless Communications Engineers and Technicians, the Private Systems Users Alliance, the Mobile Wireless Communications Alliance, and the Wireless Broadband Alliance. As the FCC-appointed frequency coordinator for the 450-512 MHz bands in the Business Radio Service, the 800 MHz and 900 MHz Business Pools, the 800 MHz General Category frequencies for Business Eligibles and conventional SMR systems, and the 929 MHz paging frequencies, PCIA represents and serves the interests of tens of thousands of FCC licensees.

² Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Further Notice of Proposed Rulemaking*, FCC 98-282 (rel. Nov. 5, 1998) ("Notice").

³ Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified in sections of 18 U.S.C. and 47 U.S.C. §§ 1001, *et seq.*).

assistance capability requirements beyond the narrow requirements that Congress described in drafting Section 103. As discussed below, PCIA supports the telecommunications industry's codification of these requirements in J-STD-025. Accordingly, PCIA urges the Commission to implement J-STD-025 as written. PCIA also responds to other proposals and questions articulated by the FCC as they relate to the agency's overall approach to CALEA compliance matters.

I. INTRODUCTION

Congress enacted CALEA in response to claims by law enforcement officials that their ability to engage in court ordered electronic surveillance had been compromised by the introduction of digital switching and transmission equipment by telecommunications carriers.⁴ In particular, law enforcement asserted that the use of these digital technologies had made it difficult, if not impossible, for them to simply tap directly into the local loop of the subject of a surveillance warrant. CALEA now requires telecommunications carriers, pursuant to a valid electronic surveillance warrant, to meet the "assistance capability requirements" by providing law enforcement officials with call content information and call identifying information that is reasonably available to the carrier.⁵ In addition, CALEA requires telecommunications carriers and manufacturers to cooperate in the development of switching and network equipment that is capable of providing law enforcement officials with this information.⁶ Finally, CALEA permits

⁴ 140 Cong. Rec. H-10779 (Oct. 7, 1994) (statement of Rep. Hyde).

⁵ 47 U.S.C. § 1002.

⁶ 47 U.S.C. § 1005.

industry associations or standards setting organizations to promulgate technical standards for CALEA-compliant telecommunications equipment.⁷ If a carrier deploys equipment that is manufactured in accordance with these standards, it must be deemed to be in compliance with the assistance capability requirements.⁸

After the passage of CALEA, members of the telecommunications industry selected the Telecommunications Industry Association (“TIA”), an ANSI-accredited institution, as its Section 107(a)(2) “industry association or standard-setting organization” for two-way voice telephony.⁹ Beginning in 1995, TIA worked with representatives of the telecommunications industry and representatives of the law enforcement community to produce a technical standard that would satisfy the assistance capability requirements. Finally, after protracted inter-industry negotiations and discussions with law enforcement officials, on December 8, 1997, TIA and the Alliance for Telecommunications Industry Solutions (“ATIS”) jointly published interim standard J-STD-025.

Since that time, this standard has been attacked as both over-inclusive and under-inclusive. In particular, the Center for Democracy in Technology (“CDT”) claimed that J-STD-025, by granting law enforcement officials access to location information and packet data, is over-inclusive.¹⁰ Alternatively, the Department of Justice (“DOJ”) and the Federal Bureau of Investigation (“FBI”) claimed that J-STD-025 did not provide law enforcement officials with

⁷ 47 U.S.C. § 1006.

⁸ *Id.*

⁹ 47 U.S.C. § 1006(a)(2).

¹⁰ Center for Democracy and Technology, Petition for Rulemaking Under Sections 107 and 109 of CALEA (filed March 26, 1998).

sufficient call identifying and call content information, and developed a “punch list” of specific features to be added to J-STD-025 in order to make it consistent with what they believed were the mandates of CALEA.¹¹

On April, 20, 1998, the Commission sought comment on the DOJ/FBI Petition and the CDT Petition, and specifically asked whether J-STD-025 met the assistance capability requirements of CALEA.¹² In that proceeding, PCIA and virtually every other commenter clearly demonstrated that the TIA-approved standard was fully consistent with CALEA, and that the “punch list” items were not statutorily mandated.

In this proceeding, the Commission again seeks to reconcile the divergent views over the adequacy of J-STD-025, to determine definitively which features must be included in this standard, and to determine to which services this standard must apply. As described in greater detail below, PCIA continues to believe that J-STD-025 has accurately translated the assistance capability requirements of CALEA to a technical standard for two-way voice telephony.

¹¹ DOJ and FBI, Joint Petition for Expedited Rulemaking (filed March 27, 1998). The punch list items are: (1) content of the conversations of all parties on conferenced calls, even after the subscriber has dropped off or been put on hold; (2) messages indicating whether a party is connected to a multiparty call at any given time (*i.e.*, “party hold,” “party join,” “party drop” messages); (3) access to subject-initiated dialing and signaling activity (*e.g.*, hold, transfer, flash); (4) notification message for network generated in-band and out-of-band signaling (*e.g.*, ringing, busy signals, call waiting signals); (5) timing to correlate call data and call content information; (6) surveillance status message, which would verify that the surveillance is on the correct service and is operational; (7) feature status message, which would report any changes in a subscriber’s service features; (8) continuity tone or signal, which would ensure that law enforcement is notified immediately if the delivery channels from the carrier have failed; and (9) post cut-through dialing and signaling information delivered on the call data channel. *See Id.* at 27-59.

¹² Public Notice, *Communications Assistance for Law Enforcement Act*, CC 97-213, DA 98-762 (April 20, 1998).

Therefore, the Commission should not add any of the “punch list” items sought by law enforcement officials, and deem J-STD-025, in its present form, to be a legally sufficient basis for manufacturing CALEA-compliant equipment.

Finally, because messaging services and other communications services operate under different technological and regulatory constraints than two-way voice telephony, J-STD-025 is not applicable to these other industries. The paging and SMR industries, for example, continue to develop their own service specific standards consistent with language of CALEA.¹³ Representatives of those services continue to apprise the Commission of their progress and those activities should not be impacted by this proceeding.

II. THE ASSISTANCE CAPABILITY REQUIREMENTS ARE TO BE INTERPRETED NARROWLY AND IN A MANNER THAT PROTECTS THE PRIVACY OF THE AMERICAN PUBLIC

The Commission first seeks comment on how it should approach its task of interpreting the assistance capability requirements of CALEA.¹⁴ As the Commission recognizes in the *Notice*, Congress clearly expected “industry, law enforcement and the FCC to narrowly interpret the requirements” of CALEA.¹⁵ In setting forth this expectation, Congress specifically explained that it did not want the Commission to engage in an “overbroad interpretation of the [assistance capability] requirements.”¹⁶ Therefore, if it is unclear whether a particular capability should be

¹³ 47 U.S.C. § 1006.

¹⁴ *Notice*, ¶¶ 23-35.

¹⁵ *Notice*, ¶ 25 (citing *Communications Assistance for Law Enforcement Act*, H.R. Rep. No. 103-827, at 23 (1994) (“House Report)).

¹⁶ House Report at 22.

included in the technical standard, Congress has suggested that the public interest should be resolved in favor of not granting the capability.

Congress further specifically noted the Director of the FBI's concession that "the legislation was intended to preserve the *status quo* [and] was intended to provide law enforcement no more and no less access to information than it had in the past."¹⁷ This is a critical yardstick by which to measure the interpretation of the assistance provisions. Again, if a question is close or not clear, the Commission should look to see if its interpretation of the provision would result in law enforcement officials obtaining access to information that they do not currently enjoy.

Both the text and the legislative history of CALEA further demonstrate a clear Congressional intent to strike a compromise between: (1) the needs of law enforcement officials, pursuant to a valid warrant, to access certain call content and call identifying information; and (2) the Constitutional right of the American people to engage in electronic communications without governmental surveillance. Carriers are required to "protect the privacy and security of communications and call identifying information not authorized to be intercepted" when releasing call content and call identifying information to law enforcement officials.¹⁸ In addition, in evaluating the adequacy of technical standards, the Commission is required to "protect the privacy and security of communications not authorized to be intercepted."¹⁹ Similarly, in determining whether compliance with CALEA's technical standards is reasonably achievable for

¹⁷ *Id.*

¹⁸ 47 U.S.C. § 1002(b)(4)(A).

¹⁹ 47 U.S.C. § 1006(b)(2).

post-1995 equipment, the Commission is told to evaluate, *inter alia*, “the need to protect the privacy and security of communications not authorized to be intercepted.”²⁰

The legislative history of the Act confirms the importance of protecting the American people from unauthorized surveillance while still accommodating the legitimate needs of law enforcement agencies. In particular, in enacting CALEA, Congress stated that “for the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement.”²¹ Further, the House and Senate Judiciary Committees noted that “as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.”²²

Against this statutory background, the Commission must define “call identifying information” and “reasonably available” in a manner that protects the American people from unauthorized electronic eavesdropping. The best way for the Commission to carry out this mandate is to interpret these terms as narrowly as possible, so that law enforcement officials are not provided with more information than Congress intended.

III. THREE CRITICAL COMPONENTS OF THE ACT MUST GUIDE THE COMMISSION’S ANALYTICAL APPROACH TO EACH FEATURE OF THE PUNCHLIST

In determining whether any of the features of the punch list are mandated by the assistance capability requirements of Section 103, the Commission must undertake a three-step analysis. First, the Commission must determine whether the feature calls for the provision of

²⁰ 47 U.S.C. § 1008(b)(1)(C).

²¹ House Report at 11.

²² *Id.* at 17.

“call identifying information” within the meaning of Section 102 of CALEA. Second, if the feature does call for the provision of such “call identifying information,” the Commission must determine whether this information is “reasonably available to the carrier.”²³ Finally, even if the feature in question calls for the provision of reasonably available call identifying information, the Commission must determine whether the feature is mandated by the multi-factor test of Section 107(b).

A. Call Identifying Information

In its analysis of the different capability requirements, the Commission must first address the issue of whether the information requested is, indeed, call identifying information. The Act defines “call identifying information” as “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber.”²⁴ For voice communications, the legislative history goes on to define “call identifying information” as “electronic pulses, audio tones, or signaling messages that *identify the numbers* dialed or otherwise transmitted for the purpose of routing calls through the carrier’s network.”²⁵ For pen register investigations, the legislative history defines “call identifying information” as “*the numbers* dialed from the facility that is the subject of the court order.”²⁶ And, for trap and trace devices, “call identifying information” is defined as “*the originating*

²³ 47 U.S.C. § 1002(a)(2).

²⁴ 47 U.S.C. § 1001(2).

²⁵ House Report at 21 (emphasis added).

²⁶ *Id.* (emphasis added).

number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order.”²⁷

Thus, it is clear that in requiring carriers to provide law enforcement officials with “call identifying information,” Congress wanted to ensure that law enforcement officials were provided with the telephone numbers dialed by the subject of a warrant from his or her telephone and the telephone number associated with a call coming into the telephone of the subject of a warrant. Defining “call identifying information” in such a manner is further consistent with the intent of Congress to define the assistance capability requirements narrowly, in a such a manner that does not alter the *status quo* in favor of expanding the electronic surveillance capabilities of law enforcement agencies.

B. “Reasonably Available” Includes an Element of Cost Determination

Even if a requested feature does indeed provide a law enforcement agency with call identifying information, the inquiry as to whether such a feature is required under CALEA is not complete. The next finding the Commission must make is “whether the information to be provided to a law enforcement agency under Section 103(a)(2) is *reasonably available* to the carrier.”²⁸ While the word “available” is not defined in CALEA, the dictionary defines this term as “accessible for use; at hand.”²⁹

Given enough resources and time, of course, almost any type of information that passes through the switch could be made “accessible for use” by law enforcement agencies. Congress

²⁷ *Id.* (emphasis added).

²⁸ *Notice*, ¶ 25 (emphasis added).

²⁹ Webster's II New Riverside University Dictionary 141 (1988).

therefore sensibly tempered the word “available” by requiring that it be “reasonably” available. Like “available,” the term “reasonably” is not specifically defined in the Act, and the legislative history concerning this qualifier is rather sparse. As the Commission noted in other contexts, however, in cases where the definition of a term is ambiguous, the FCC must “consider the statutory context in which the term is used to give it precise meaning.”³⁰

Preliminarily, as discussed above, the Commission should define “reasonably available” narrowly, in a manner that does not provide law enforcement agencies with capabilities beyond what they currently enjoy, and preserves customer privacy to the greatest extent possible. One means of implementing this requirement would be through the use of burdens of proof. In particular, if a law enforcement agency argues that a carrier is not in compliance with or is failing to provide an assistance capability, it would be incumbent upon the law enforcement agency to demonstrate that the capability it seeks is “reasonably available” from the standpoint of the carrier. By requiring law enforcement agencies to make this showing, the Commission will ensure that the assistance capability requirements are not given an overly expansive interpretation.

A second context is provided in Section 109, in which Congress outlined several factors it wanted the Commission to consider when examining whether a capability was “reasonably achievable.”³¹ As mentioned above, with enough resources, nearly any type of capability is “achievable.” Congress, however, sought to limit the reach of that term by requiring that the

³⁰ AT&T Corp. v. Ameritech, *et al.*, File Nos. E-98-41, *et al.*, *Memorandum Opinion and Order*, FCC 98-242, at ¶ 28 (rel. Oct. 7, 1998).

³¹ See 47 U.S.C. § 1009.

capability be “reasonably achievable” and outlining several different factors it wanted the Commission to examine. Section 109 therefore defines the word “reasonable” for the purposes of CALEA in the context of examining and evaluating capability requirements. Thus, while Section 103 has no such list defining “reasonability,” the Commission should not hesitate to use the factors found in Section 109 to make that determination. By so doing, the Commission will be faithfully looking to the context of CALEA to define an ambiguous term.

In the *Notice*, the Commission also requested comment on the relevance of cost in the context of “reasonable availability.”³² Given the aforementioned relationship between Sections 103 and 109, the Commission only need look to the factors in Section 109 to determine the role that cost should play. An examination of these factors reveals that several of the criteria listed (Section 109(1)(B), (D), (E), (H)) either directly or indirectly concern the price of the technology or the overall effect of the cost on carriers. Thus, cost plainly must play an important role in the Commission’s evaluation of whether a capability is “reasonable available” under Section 103.

Against this background, the Commission must take every reasonable step to ensure that it has adequate cost data for the core features of J-STD-025 and any additional punch list items prior to adding any features to the industry standard. Further, the Commission must put this cost data out for public comment. Based on manufacturer data submitted to the Department of Justice, the Attorney General has estimated that it will cost \$2 billion dollars to implement the core standard.³³ The telecommunications industry has not, however had an opportunity to analyze, or comment on these cost estimates.

³² *Notice*, ¶ 26.

³³ *See* Letter from Attorney General Janet Reno, *et al.* to Honorable Ted Stevens (Oct. 6, 1998).

Such comment is essential in that the Commission must have hard data on the cost of J-STD-025's features prior to imposing even greater costs on the nation's ratepayers by adding the punch list items. Therefore, if the Commission cannot elicit any significant amount of cost data in this proceeding, it should undertake a new proceeding designed to obtain such information. If the Commission does take real, hard cost data into account in determining whether call identifying information is "reasonably available," in this proceeding it will be forced to do so later, when carriers file petitions under Section 109(b), claiming that compliance with the assistance capability requirements is not "reasonably achievable" due to excessive cost.³⁴

In grappling with the cost component of "reasonably available," the Commission should finally be aware of three additional issues. First, with the approach of the Year 2000, the telecommunications industry is focusing its information technology resources on ensuring that its networks deliver reliable service, and avoid any Y2K bugs. This concentration on providing seamless service into the new millennium will create a shortage of programmers and systems engineers, which will inevitably raise the cost of other information technology products that must be developed at the same time—including the development of CALEA-compliant network hardware and software.

Second, in the compliance deadlines imposed by the Commission are unlikely to coincide with any carrier's normal software update cycle. Therefore, carriers will be required to install and test CALEA-compliant software loads separately from the updates that are normally purchased from their switch vendors. Because these out-of-cycle switch upgrades will increase the cost of CALEA compliance, the Commission should give the carriers the flexibility to defer

³⁴ 47 U.S.C. § 1008(b).

installing CALEA-compliant switch software until such time as they would normally upgrade a particular switch.

Third, compliance costs will vary based on the FBI's capacity requirements, which are currently being challenged in federal court.³⁵ The Commission must be aware that the issues of capability and capacity are closely linked, as technical solutions to providing call identifying and call content information will vary in price and efficacy depending upon how many circuits carriers must reserve for law enforcement use. Therefore, in evaluating the cost data that is submitted for CALEA-compliance, the Commission should verify the capacity assumptions made by the parties submitting this data. In addition, the Commission should be prepared to re-evaluate the cost estimates based on the court's ruling on the FBI's *Final Capacity Notice*.

C. The Section 107(b) Factors Must Be Satisfied

PCIA agrees with the Commission's determination that the final step that it must make before it can establish a CALEA requirement is found in Section 107(b).³⁶ This section specifically sets forth four requirements that any technical standards must meet before being sanctioned by the Commission. Under Section 107(b), any Commission-approved standards must: (1) meet the assistance capability requirements by cost-effective means; (2) protect the privacy and security of communications not authorized to be intercepted; (3) minimize the cost of CALEA compliance on residential ratepayers; and (4) encourage the provision of new technologies and services to the public.³⁷

³⁵ See *PCIA, et al v. Reno*, Nos. 98CV01036, 98CV02010 (D.D.C. filed April 27, 1998).

³⁶ *Notice*, ¶ 29.

³⁷ 47 U.S.C. § 1006(b).

As described above, the factors that address a feature's price—ensuring that compliance occurs by cost-effective means, and minimizing the financial impact on residential ratepayers—are already incorporated into the definition of “reasonably available” call identifying information. The fact that Congress has seen fit to mention these financial factors twice, however, re-iterates the importance of compliance costs in the Commission's evaluation of any punch list item. This statutory redundancy is also consistent with the desire of Congress to prevent law enforcement officials from “gold plating” CALEA's technical standard by demanding expensive features that are useful to law enforcement, but are not required by the narrow parameters of CALEA.³⁸

Protecting the privacy of the American public is another criteria that Commission must consider in determining the adequacy of a proposed technical standard. This factor is particularly important in evaluating whether law enforcement officials should have access to greater call content and call identifying information than they have enjoyed in the past. In making this decision, the Commission should respect the reasonable expectations of privacy that Americans have enjoyed historically, and not permit the implementation of technical standards that encroach on these expectations.

Finally, the Commission is tasked with ensuring that the technical standards do not reduce the ability or incentive of telecommunications providers to offer new and innovative technologies and services to the American public. In this regard, the Commission must again consider whether the cost of implementing a particular feature demanded by law enforcement

³⁸ See 140 Cong. Rec. H10781 (Oct. 4, 1994) (Congressman Markey's statement that law enforcement officials should be prohibited from “gold-plating” their demands).

will make a new technology or service prohibitively expensive for the average American. In addition, the Commission must not permit law enforcement to add assistance capability requirements that are fundamentally incompatible with new technologies and services. This factor is particularly important in evaluating technical standards for new wireless services and packet data systems, as many of these new technologies are on the verge of roll-out, and any increase in price or decrease in features will make them less marketable.

IV. PARTICULAR CAPABILITIES OF J-STD-025 REPRESENT INDUSTRY COMPROMISE, NOT STATUTORY REQUIREMENTS

J-STD-025 represents industry's attempt, in a manner based on technical realities and reasonability, to interpret the capability requirements of the Act. In this context, there are a number of instances where the standard represents a compromise between industry's interpretation of CALEA and the interpretation of the law enforcement agencies. Thus, while J-STD-025 is an attempt to implement the assistance capability requirements of CALEA, due to the fact that it represents a compromise, the standard is not the definitive legal interpretation of the Act. In fact, in cases where industry compromised with law enforcement, it is likely that the standard may go beyond the capabilities that the Act actually requires. Thus, simply because a capability was included in a working draft of the standard or even in the standard itself does not mean that the capability is statutorily required. Instead, it simply means that industry has attempted to accommodate law enforcement while at the same time implementing the spirit of CALEA.

A. Geographic Location Information Is Not Required Under CALEA, Thus Information Derived In Other Contexts Can Be Used To Satisfy Law Enforcement's Requests

One capability that represents a compromise with law enforcement is the provision of

location information that would identify a mobile phone user's cell site location at the beginning and termination of a call. The Commission concluded that this information falls under the rubric of "call identifying information."³⁹ The provision of this information, however, is not required by the Act. First, this information does not fall under the definition of "call identifying information" because the manner by which this information would be provided to law enforcement is not through the "dialing or signaling information" that is used to route the call. Second, the provision of this information does not preserve the *status quo* and adds to the amount of information law enforcement receives. Third, carriers may not be able to provide just the cell-site location; under many E911 plans, the carrier will be providing sector location information in addition to cell site location. Separating the cell-site information thus may not be reasonably available. Therefore, the Commission's approach, contrary to the intent of Congress, broadly interprets the Act and impermissibly expands the definition of "call identifying information."

Nevertheless, if the Commission does ultimately determine that this location information is a CALEA requirement, it should permit carriers to provide law enforcement agencies with whatever location information they are required to generate in the ordinary course of their business or to comply with other Commission obligations (*i.e.*, the E911 requirements).⁴⁰ Giving carriers this flexibility is imperative, because under Section 103, a carrier is not required

³⁹ Notice, ¶ 52.

⁴⁰ Carriers may not in fact have such information available by the CALEA compliance deadline of June 30, 2000. Although Section 20.18(d)(1) of the Commission's rules states that carriers must provide cell site location (and call-back number) by April 1, 1998 (Phase I), Section 20.18(f) states that *carriers do not have to provide cell site location until the PSAP requests the information, has the capability to use the information, and there is a cost recovery mechanism in place*. Given the slow pace of Phase I implementation, it is very possible that cell site location will not be reasonably available by the CALEA deadline.

specifically to design its equipment to comply with CALEA's requirements.⁴¹ Thus, a carrier cannot be compelled to add a capability to its system that would generate information beyond that which can be provided through the carrier's existing equipment to satisfy its own internal requirements or other Commission obligations. Thus, any location information that must be provided to a law enforcement agency under CALEA can be no more than the existing location information that a carrier currently has in its switches.

B. Call Content and Call Identifying Information Must Be Narrowly and Specifically Defined In the Packet Data Context

Consistent with existing privacy law and CALEA, the Commission must be careful to define call content and call identifying information narrowly and specifically for packet data. Regardless of whether a communication is circuit switched or packet switched, CALEA prohibits carriers from providing law enforcement agencies with call content information when the law enforcement agency has only been authorized to receive call identifying information.⁴² In addition, the Commission is not authorized to modify what is meant by "call identifying information" nor is it authorized to interpret this term in a broad and sweeping fashion when dealing with packet data. Therefore, just as in the context of "traditional" methods of routing calls, call identifying information is narrowly defined as information that is used to route the call through the carrier's system.

Similarly, while in the past carriers have provided the content of packet-switched calls to law enforcement agencies pursuant to pen register or trap and trace warrants,⁴³ this past practice

⁴¹ See 47 U.S.C. § 1002(b)(1).

⁴² 47 U.S.C. § 1002(a)(4)(A).

⁴³ See Notice, ¶ 62.

does not square with the requirements that carriers are obligated to follow under CALEA.

Therefore, simply arguing that providing call content information in the packet data context is just an extension of what has always been done cannot justify extending this practice to this new technology. Instead, CALEA requires that carriers either provide separated packet headers with only the call identifying information when the law enforcement agency only has a trap and trace or pen register warrant, or not provide any call identifying information at all.

In addition, the other provisions of CALEA also govern the provision of call identifying information and call content information in the packet data environment. Specifically, any interpretation of what is “reasonably available” and “reasonably achievable” remains no different in the packet environment. Thus, the Commission will be required to minimize the effect of CALEA compliance on end-user rates. Critically, the FCC will also need to evaluate the impact of providing call content and call identifying information for packet data services on the development and deployment of new technologies and services, many of which utilize packet data transfers.

V. THE FCC’S APPROACH TO SURVEILLANCE STATUS, CONTINUITY CHECK TONE, AND FEATURE STATUS CORRECTLY COMPORTS WITH THE STATUTORY LANGUAGE AND INTENT OF CONGRESS

A. The Commission Correctly Interpreted CALEA To Find That Automated Delivery of Surveillance Status Information Is Not Required

Law enforcement agencies demand that they be provided with a “surveillance status message” that will periodically inform them that an interception is in place and functional.⁴⁴ The Commission correctly concluded in its *Notice* that “a surveillance status message does not fall

⁴⁴ See *Notice*, ¶ 106.

within any of the provisions of Section 103” because this information is not related to any specific call, and therefore cannot be classified as “call identifying information.”⁴⁵ PCIA agrees with the Commission’s analysis and adds that including surveillance status information within the definition of “call identifying information” stretches this definition far beyond what Congress intended.

In addition, even if surveillance status information could be defined as “call identifying information,” which it cannot, there is a substantial question as to whether this information is “reasonably available” to wireless carriers. In particular, because CMRS networks currently have no way of polling remote switches to ensure that they are operational, they cannot provide law enforcement officials with this information.⁴⁶ Because implementation of this feature would require wireless carriers to undergo the substantial expense of retrofitting their switching systems to make surveillance status information available, it would impose substantial costs on such carriers. Further, given the highly competitive nature of the CMRS industry, these costs would inevitably be passed onto wireless customers.

Finally, the FBI’s attempts to stretch the term “shall ensure” to include a verification capability is a significant step away from the narrow interpretation of the Act’s assistance capability requirements required by Congress. Carriers are required under the Act to provide law enforcement agencies only with access to call content and call identifying information. They are

⁴⁵ See *Id.*, ¶ 109.

⁴⁶ See Telecommunications Industry Association Comments in CC Docket No. 97-213, at 70 (dated May 20, 1998).

forbidden from providing “information not authorized to be intercepted.”⁴⁷ Because providing law enforcement agencies with a means of continual and constant verification is neither call content nor call identifying information, the FCC’s interpretation honors the Congressional command that it interpret CALEA as narrow as possible regarding these assistance requirements.

B. The Commission’s Conclusion Regarding the Check Tone Correctly Applies the Section 103 Factors

Another “punch list” item is a requirement that carriers provide law enforcement officials with a “continuity tone” to ensure that the call content channels between the carrier and law enforcement officials are in good working order.⁴⁸ As in the case of surveillance status information, the Commission’s conclusion “that this technical requirement is not necessary to meet the mandates of Section 103(a)” is correct.⁴⁹ Because this information is not call specific and does not lead to the generation of any call identifying information, it cannot be deemed a capability requirement under any reasonable reading of the Act.

Further, check tone information is not reasonably available to carriers. Specifically, when wiretaps were local loop-based, *law enforcement* officials used to send a “C-tone” over the local loop to ensure that the call content channels were operative. CALEA, however, contemplates that carriers will implement the assistance capability requirements in a switch-based manner. Therefore, in order to implement this “punch list” item, *carriers* would be required to install C-tone generators at the switch level. Given that a continuity check is not

⁴⁷ 47 U.S.C. § 1002(A)(4)(a).

⁴⁸ *Notice*, ¶ 111.

⁴⁹ *Id.*, ¶ 114.

required by CALEA, there is certainly no reason to require carriers—and ultimately ratepayers—to underwrite its considerable expense.

C. The Commission's Conclusion Regarding the Provision of Feature Status Further Advances the Intent of Congress

In the “punch list,” law enforcement agencies further requested that carriers send law enforcement officials a real time message indicating which calling features and services (*e.g.*, call waiting, call forwarding) the subject of a surveillance warrant has implemented.⁵⁰ Like the aforementioned two features, this feature is not required by Section 103 because it is not call identifying information. As the Commission accurately notes, these messages “do not pertain to the actual placement or receipt of individual calls” and “are not necessary to intercept either wire or electronic communications on a carrier’s system.”⁵¹ Thus, the Commission is correct in concluding “that the feature status punch list item does not meet the assistance capability requirements of Section 103.”⁵²

Further, this information is not reasonably available to carriers, as they do not maintain a real-time database of which features have been implemented by which customers at any given time. It would in fact be tremendously expensive for the nation’s telecommunications carriers to generate on-line service profiles for each of their customers solely to serve the needs of law enforcement officials. Again, carriers will have no choice but to pass these implementation costs onto their customers. As such, deployment of this feature should be flatly prohibited by Section

⁵⁰ *Id.*, ¶ 116.

⁵¹ *Id.*, ¶ 121.

⁵² *Id.*

107(b)(3)'s command that the Commission "minimize the cost of such compliance on residential ratepayers."⁵³

Finally, law enforcement officials can already obtain this information by simply serving the subject's carrier with a subpoena. Therefore, a cost-effective method of providing law enforcement officials with a list of a subject's features already exists. Under such circumstances, the Commission should not impose this costly mandate on carriers.

VI. THE FCC'S APPROACH TO THE REMAINING "PUNCH LIST" ITEMS IS INCONSISTENT WITH THE STATUTORY LANGUAGE AND INTENT OF CONGRESS

A. The Content of Conference Calls Can Only Be Provided When the Subject Remains Part of the Call.

The Commission tentatively concluded that the Act requires carriers to provide the content of subject-initiated conference calls, even when the subject has dropped off the call.⁵⁴ Because this capability is not required by Section 103, impermissibly impinges upon the privacy of the American public, and is not reasonably achievable, it should not be included in the final standard.

First, under Section 103, carriers are only required to provide call content information that is "carried by the carrier within a service area *to or from equipment, facilities or services of a*

⁵³ 47 U.S.C. § 1006(b)(3).

⁵⁴ *Notice*, ¶ 77. It is important to note that J-STD-025 already provides law enforcement officials with the ability to eavesdrop on the conversations of all participants to a conference call as long as the subject of the warrant, or someone using the subject's phone remains connected to the call.

subscriber of such carrier.”⁵⁵ Once the subscriber—or subject of the warrant—has either hung up, or placed the other parties on hold, the content of the call is no longer going *to* that subscriber’s equipment, facilities, or services. Instead, at the very most, the content could be going *through* the subscriber’s equipment. In other words, because the subscriber’s equipment is no longer a termination point, but a conduit, this capability is not within the assistance capability requirements of Section 103.

In addition, the FBI/DOJ concedes that J-STD-025’s treatment of conference calls “does not amount to a reduction in the information that has been available to law enforcement.”⁵⁶ Therefore, given that the assistance capability requirements were “intended to provide law enforcement with no more and no less access to information than it had in the past,”⁵⁷ the Commission’s tentative conclusion would upset the current *status quo*. Therefore, the Commission should not require carriers to provide call content information when the subject has dropped off of the conference call.

Section 103 of CALEA further obligates carriers to “protect[] the privacy and security of communications and call identifying information not authorized to be intercepted.”⁵⁸ If carriers are required to provide law enforcement officials with this punch list item, it could be argued that they are violating their obligation to ensure customer privacy. In particular, once the subject of the warrant has dropped off the call, the carrier will be facilitating the *warrantless* electronic

⁵⁵ 47 U.S.C. § 1002(a)(1) (emphasis added).

⁵⁶ DOJ and FBI Joint Petition for Expedited Rulemaking at 30.

⁵⁷ House Report at 22-23.

⁵⁸ 47 U.S.C. § 1002(a)(4).

surveillance of the other parties on the conference call. This result cannot be squared with the requirement that carriers only permit wiretapping pursuant to a court order that “identif[ies] the person, if known, whose communications are to be intercepted” and “the place where authority to intercept is granted.”⁵⁹ If the law enforcement agencies wish to monitor the conversations of those parties remaining on the line, they are statutorily required to obtain warrants allowing them to do so.

The Commission’s approach also represents an expansive interpretation of the term “facilities” in the Act, contrary to Congressional intent. Again, because this term is not specifically defined in CALEA, its meaning must be ascertained by examining the Act’s context. In this instance, PCIA concurs with TIA’s approach of examining the “facilities” doctrine of Title III to define this term and agrees with TIA’s conclusion that granting this capability request as part of the “punch list” impermissibly expands the scope of CALEA. As TIA points out, the term “facilities” in the context of electronic intercepts means “the actual telephone or other physical facilities of the intercept subject”—not the entire network to which the telephone is attached.⁶⁰ Taking law enforcement’s approach to its logical conclusion, once a target dialed into the public switched network, the *entire* network would be fair game for interception because it would become part of the target’s “facilities.” This expansion of the term “facilities” is clearly far beyond the realm of anything Congress envisioned, and should not be endorsed by the Commission.

⁵⁹ See 18 U.S.C. §§ 2518(1)(b), (4)(a), (b).

⁶⁰ TIA Comments at 35.

Finally, this information is not reasonably available to carriers because accessing this data will be very expensive. In this regard, the Commission should not require ratepayers to subsidize what amounts to “gold-plating” on the part of law enforcement officials.⁶¹

B. Party Hold, Party Join, Party Drop Messages For Multi-Party Calls Are Not “Call Identifying Information”

In the *Notice*, the Commission tentatively concluded that “party hold/join/drop information ... is a technical requirement that meets the assistance capability requirements of Section 103.”⁶² This conclusion is based on the Commission’s tentative finding that this information “falls within CALEA’s definition of ‘call identifying information’” because it is signaling information that directs a call.⁶³ PCIA respectfully disagrees.

Party hold/join/drop information is not “call identifying information” within the definition and intent of CALEA. Specifically, when a party acts to join, hold, or drop during the course of a multi-party call, that party is not generating “call identifying information,” which is defined as signaling information that identifies either: (1) “the numbers dialed or otherwise transmitted for the purpose of routing calls through the carrier’s network;” (2) “the numbers dialed from the facility that is the subject of the court order;” or (3) “the originating number of

⁶¹ See 140 Cong. Rec. H10781 (Oct. 4, 1994) (Congressman Markey’s statement that law enforcement officials should be prohibited from “gold-plating” their demands).

⁶² *Notice*, ¶ 86. Of note, J-STD-025 already provides law enforcement officials with information that “substantially satisfies” the “party join” and “party drop” capabilities. J-STD-025 requires that carriers notify law enforcement of “Termination/Attempt” and “Change” messages which indicate when a party joins a multi-party call supported by the subscriber’s facilities, and provide the “Release” message which notifies law enforcement when a party is dropped from a multi-party call.

⁶³ *Notice*, ¶ 85.

the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order.”⁶⁴ Instead, this signaling information relates to the specific status of a party to the conference call that may or may not be directed to the subject of the court order. Thus, because this hold/join/drop information is not “call identifying information,” it is not encompassed within the assistance capability requirements of Section 103.

Again, the Commission’s approach represents a prohibitively broad interpretation of the Act that does not comport with Congress’ idea of “call identifying information” as focusing on the numbers used to route a call. In particular, a signal regarding a party’s particular status on a multi-party call is not the information that is used to route the call. Further, interpreting the capability requirement in such a manner would provide law enforcement with information that they do not currently receive⁶⁵—in contravention of Congress’ intent to maintain the *status quo*.

The rationale advanced by law enforcement to obtain this information is also without merit. The FBI claims that this information is necessary to determine who heard what during the course of a conversation. As TIA notes, however, “party hold” information does not eliminate any uncertainty regarding who actually heard what during the course of a conference call because a party could walk away from a phone during the conference. The mere fact that a party was not on hold, with nothing more, does not sufficiently establish the fact that a party heard a statement during a multi-party call, especially in light of the high burdens of proof and persuasion that the government must meet in a criminal trial. Indeed, TIA is correct in its assertion that the only legally sufficient evidence of participation in a conference call would be some sort of response

⁶⁴ House Report at 21.

⁶⁵ See Notice, ¶ 81 (citing Comments of AT&T).

by the party alleged to have participated. Therefore, given the lack of value of this party hold/join/drop information, the Commission should not distort the Act in the manner advanced by the law enforcement agencies.

In any event, if any of these hold/join/drop features are implemented through the party's customer premise equipment ("CPE"), then the status of the party will not be detected by the network. The Commission itself has correctly stated in the *Notice* that if such features are provided by a subject's CPE, that "information could not be reasonably made available to the LEA, since no network signal would be generated."⁶⁶

C. Subject-Initiated Signaling Information Does Not Fall Under CALEA's Requirements

Providing subject-initiated signaling information would require carriers to forward to law enforcement officials information detailing when a subject uses services such as call waiting, call forwarding, call hold, and three-way calling. Contrary to the Commission's tentative conclusion, however, subject-initiated dialing and signaling activity (*e.g.*, hold, transfer, flash) is not "call identifying information" within the meaning of CALEA.⁶⁷ Just as in the case of hold/drop/join information, when the subject of a warrant depresses the telephone's hook or presses the "flash" key, presses the "hold" key, or presses the "transfer" key, he or she is not generating signaling information that identifies either: (1) "the numbers dialed or otherwise transmitted for the purpose of routing calls through the carrier's network;" (2) "the numbers dialed from the facility that is the subject of the court order;" or (3) "the originating number of the facility from which

⁶⁶ *Notice*, ¶ 86.

⁶⁷ *Id.*, ¶ 94.

the call was placed and which are captured when directed to the facility that is the subject of the court order.”⁶⁸ Instead, this signaling initiates features of the subject’s telephone account. Because this subject-initiated signaling activity falls outside of the parameters Congress intended the term “call identifying information” to cover, it cannot be a required CALEA capability.

Further, even if this feature were mandated by Section 103, it is far from clear that such information is currently readily available to carriers or could be made available in a cost-effective manner. In particular, in some switches, detection and collection of off-hook indicators occurs in a “line module” that is separate from the main processor of the switch. Therefore, making this information available to the main processor so that it can be sent to law enforcement may require fundamental, and expensive, modifications to switch design.

D. Network-Generated In-Band and Out-of-Band Signaling

This capability would require a carrier to notify a law enforcement agency when any type of network message (*e.g.*, a call waiting tone, a busy signal, or a ringing indicator) is sent to the subject’s phone. Law enforcement officials claim they are entitled to this information because it is signaling information that can be sensed by the subject, and, therefore, is important to preventing crime.⁶⁹ The Commission, tentatively agreed, concluding that such signals do, indeed, “constitute call identifying information under CALEA,” and, thus is a required capability.⁷⁰

⁶⁸ House Report at 21.

⁶⁹ *Notice*, ¶ 98.

⁷⁰ *Id.*, ¶ 99.

Because this feature will not provide “call identifying information” within the meaning of Section 103, it should not be included in the final standard. As discussed in previous sections, “call identifying information” is specifically defined as information that is used to route calls to or from the subject’s phone. These network messages are not used to route calls, but merely inform the subject as to the status of calls made or received. In addition, providing law enforcement officials with all in-band and out-of-band signaling information would represent a significant expansion of law enforcement’s historic ability to engage in electronic surveillance. Therefore, the Commission should reconsider its tentative conclusion, bearing in mind that carriers are under an obligation to protect user privacy, and under *no* obligation to provide law enforcement officials with information about what the subject knows, and when he or she knows it.

While the in-band and out-of-band signaling information requested by law enforcement agencies is not required under the Act, the telecommunications industry *has* agreed, in J-STD-025, to provide the following information to law enforcement. First, the “Termination/Attempt” message defined in J-STD-025 alerts law enforcement at the time of each incoming call.⁷¹ Second, J-STD-025 provides the following data that reflects “audible signaling information:” (1) the number dialed and whether the call was answered;⁷² (2) call-waiting signals;⁷³ (3) call-forwarding reminders;⁷⁴ and (4) information that an incoming call was not answered.⁷⁵ Third,

⁷¹ See J-STD-025 § 5.4.10.

⁷² See J-STD-025 § 5.4.1 (Answer message), § 5.4.5 (Origination message).

⁷³ See J-STD-025 § 5.4.10 (Termination/Attempt message).

⁷⁴ See J-STD-025 § 5.4.7 (Redirection message).

visual signals of incoming calls or messages (*e.g.*, call waiting lights) certainly are not call identifying information. J-STD-025, however, informs law enforcement officials that there was an incoming call, the number at which it originated, and the fact that it was unanswered.⁷⁶ Fourth, and finally, the Termination/Attempt message included in J-STD-025 provides law enforcement officials with the calling party number, thereby providing the equivalent of an “alphanumeric” CallerID readout.⁷⁷

These features should be sufficient to provide law enforcement officials with the information they need. The Commission should therefore be wary of any attempt by law enforcement officials to gain access to additional signaling data not authorized by CALEA.

E. Timing of Call Identifying Information

Law enforcement agencies make two specific requests regarding the timely delivery of call identifying information. First, they demand that call identifying information be delivered to law enforcement within three seconds of the event that created the information.⁷⁸ Second, they demand that events be time stamped to an accuracy of 100 milliseconds.⁷⁹ The Commission

(...Continued)

⁷⁵ See J-STD-025 § 5.4.1 (Answer message), § 5.4.10 (Termination/Attempt message).

⁷⁶ See J-STD-025 § 5.4.10 (Termination/Attempt message), § 5.4.1 (Answer message).

⁷⁷ See J-STD-025 § 5.4.10 (Termination/Attempt message).

⁷⁸ See Notice, ¶ 101.

⁷⁹ *Id.*

granted law enforcement's request, reaching a tentative conclusion that "time stamp information fits within the definition of call identifying information with section 102(2) of CALEA."⁸⁰

Because these specific capabilities are not required by CALEA, they should not be included in the final standard. Regarding the timely delivery of information, the Commission concedes "that CALEA does not impose a specific timing requirement on carriers."⁸¹ In particular, Section 103 only requires carriers to deliver reasonably available call identifying information "before, during, or *immediately after* the transmission of a wire or electronic communication."⁸² The industry's proposed standard, J-STD-025, reflects the mandates of Section 103 by requiring carriers to deliver call identifying information to law enforcement officials as soon as it is generated, except where the call data channel becomes congested.⁸³ Thus, J-STD-025's handling of this information is timely in that call identifying information is passed on to law enforcement officials either "during or immediately after" the call, except when there are an insufficient number of call data channels.⁸⁴ Under such circumstances, however, law enforcement officials can simply lease more channels.

A requirement that call data channel messages be time stamped within a specified time period of their occurrence is similarly not required by Section 103. In fact, this section merely requires that reasonably available call identifying information be provided "in a manner that

⁸⁰ Notice, ¶ 104.

⁸¹ *Id.*

⁸² 47 U.S.C. § 1002(a)(2)(A) (emphasis added).

⁸³ See J-STD-025 §§ 4.4, 4.6.2 (Call-Identifying Information IAP)

⁸⁴ See *id.*

allows it to be associated with the communication to which it pertains.”⁸⁵ Because J-STD-025 associates call identifying information with the phone call to which it belongs, the standard fully comports with the Act.

Finally, this information—in the format requested by law enforcement agencies—is not reasonably available to carriers under the present configuration of the telephone network. Thus, carriers would be required to reconfigure their networks in order to provide this information. Carriers cannot be required to make this effort because not only would this reconfiguration be tremendously expensive, but the Act specifically does not require carriers to undertake such modifications.⁸⁶

F. Post-Cut-Through Dialing Information Delivered Over The Call Data Channel

Post-cut-through dialing information consists of the numbers dialed by a caller after a call circuit has been completed by the carrier that is carrying out an intercept order. These post-cut-through numbers can be used to interact with: (1) interactive information systems; (2) credit card billing services; (3) paging systems; and (4) an interexchange carrier’s network. In the *Notice*, the Commission mistakenly concluded “that post-cut-through digits representing all telephone numbers needed to route a call [and are therefore] are call identifying information.”⁸⁷

⁸⁵ 47 U.S.C. § 1002(a)(2)(B).

⁸⁶ See 47 U.S.C. § 1002(b)(1)(A) (CALEA “does not authorize any law enforcement agency ... to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any” carrier).

⁸⁷ *Notice*, ¶ 128.

This conclusion is erroneous for a number of reasons. First, post-cut-through numbers are not “call identifying information” for the originating carrier because they do not identify “the origin, direction, destination, or termination”⁸⁸ of the call. As far as the originating carrier is concerned, the call has already been connected, or “cut-through” to the second carrier. Second, even if these numbers were call identifying information, they are not “reasonably available” to the originating carrier. In particular, because switches detect dialed digits with a “tone receiver,” and these tone receivers are only used until a call is completed, as the telephone network is currently configured, the originating has no access to post-cut-through digits. The alternatives, deploying significantly more tone receivers, or extracting these digits from the call content channel and then feeding them into a call data channel, are neither cost-effective nor efficient. Deploying more tone receivers will be particularly expensive in areas where the FBI has mandated large capacity requirements.

Third, not all of the digits dialed in this manner are phone numbers used to route a call. In some instances—such as when the caller is utilizing an interactive information system—these dialed digits are considered call-content information. In these cases, CALEA prohibits carriers from disclosing this information without a full Title III warrant.⁸⁹

Finally, the industry has proposed a reasonable and cost-effective alternative that protects subscriber privacy. Under J-STD-025, law enforcement officials would be provided with post-cut through digits if they serve the subscriber’s local exchange (or other originating) carrier with

⁸⁸ 47 U.S.C. § 1001(2).

⁸⁹ See 18 U.S.C. § 3121(c) (“A government agency authorized to install and use a pen register ... shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information used in call processing”).

a Title III (call content) warrant and arrange for the provisioning of a call content channel from the carrier, *or* serve the subscriber's interexchange carrier with a pen-register warrant and arrange for the provisioning of a call data channel from the carrier. Given the availability of this alternative, the Commission should not expand J-STD-025 in a manner that conflicts with Section 103 of CALEA.

VII. THE COMMISSION SHOULD CONTINUE ITS EXISTING ROLE IN ASSISTING THE INDUSTRY IN SETTING FUTURE CALEA CAPABILITY STANDARDS, BUT SHOULD NOT IMPOSE J-STD-025 BEYOND THE WIRELINE AND BROADBAND CMRS INDUSTRIES

In its *Notice*, the Commission sought comment on "what role, if any, the Commission can or should play in assisting those telecommunications carriers not covered by J-STD-025 to set standards for, or to achieve compliance with, CALEA's requirements."⁹⁰ PCIA believes that the Commission should continue its existing role in assisting the various industry segments not affected by J-STD-025 in setting CALEA standards. These industry segments include paging, SMR, and mobile satellite services.

PCIA itself has been active on the standards setting front. As noted by the Commission, on May 4, 1998, the CALEA Subcommittee of PCIA's Paging Technical Committee, with input from law enforcement officials, published version 1.0 of its CALEA Specification for Traditional Paging.⁹¹ Similarly, on August 25, 1998, PCIA's CALEA Subcommittee published version 1.0 of its CALEA Specification for Advanced Messaging. The CALEA Subcommittee is currently developing a technical standard for Ancillary Services. Messaging providers whose facilities and

⁹⁰ *Notice*, ¶ 141.

⁹¹ *Id.*, ¶ 137.

services comply with these standards, and manufacturers that build messaging equipment according to these standards will therefore be within the safe harbor formed by Section 107(a)(2) of CALEA, and, as such, should be immune from any court actions to enforce compliance with the assistance capability requirements.

The Commission played a valuable advisory role in the development of those standards by making Commission staff available for status conferences with industry and by encouraging cooperation between law enforcement and wireless representatives. In order to encourage other industry segments to establish safe harbor standards, the Commission should continue to make its legal and technical expertise available to the pertinent industry associations. Commission staff could be of particular use in informally mediating disputes between industry members and law enforcement officials regarding which features have been included in a given industry standard. Such informal mediation can avoid protracted disputes like the current proceeding which significantly delayed implementation of CALEA.⁹²

The Commission further asked what effect its decisions regarding J-STD-025, and, in particular, its decisions regarding law enforcement access to packet data and location information, should have on “the requirements and standards already adopted or currently being established by these other industry segments.”⁹³ PCIA submits that technological considerations

⁹² PCIA notes that the FBI has yet to publish law enforcement’s capacity requirements for the paging industry. Although some technical requirements are in place today and others are nearing completion, it has been established by several commenters in this proceeding that manufacturers need at least 18 months to implement changes to their products to comply with CALEA requirements. Carriers then need at least six months to deploy the CALEA-compliant equipment once it is commercially available. Accordingly, even if a paging capacity notice were issued today, paging carriers would not be able to purchase and install the compliant equipment in time to meet the September 2000 deadline.

⁹³ *Id.*, ¶ 141.

and the text of CALEA itself demand that the effects of the Commission's decisions in this proceeding should only be binding on wireline, cellular, and broadband PCS carriers, and the manufacturers of equipment used by these providers.

In particular, the Commission should not apply the J-STD-025 punch list items or any other assistance capability requirements to other industry segments because they are not necessarily applicable. This point can best be demonstrated by comparing the Commission's rationale in determining that location information falls within the scope of CALEA with the realities of the paging industry. In its *Notice*, the Commission tentatively concludes that location information is reasonably available to telecommunications carriers, in part, because location information is already available through wireless carriers' billing, hand-off, and system use features.⁹⁴ The Commission also notes that broadband wireless carriers will be required to have a location information capability as part of their E911 obligations.⁹⁵

In contrast, location information is not reasonably available to paging providers because paging networks differ technically from cellular or broadband PCS networks, and paging providers are not subject to the same regulatory regime as broadband CMRS providers. As a matter of FCC regulation, because paging carriers are not subject to the E911 mandates, the paging industry is under no existing regulatory requirement to determine, let alone provide, location information. Technically, most paging carriers broadcast messages to all of their subscribers and operate on far fewer broadcast towers than their two-way voice counterparts. As a result, most paging carriers cannot provide location to the same level of granularity as cellular

⁹⁴ *Id.*, ¶ 56.

⁹⁵ *Id.*

or broadband PCS carriers. In the context of two-way paging, paging units transmit using a timing method called ALOHA which prevents and overcomes collisions between the transmissions of different devices in the same area. Many base station receivers can, and normally do, receive messages from the same paging device. Thus, a message could be received by a relatively distant receiver or receivers. As a result, location of the receiver or receivers will not indicate where the subscriber is, except in a very general way. Thus, location information has not been incorporated into the suite of standards developed by the paging industry.

Similarly, some of the assistance capabilities that have traditionally been delivered to law enforcement by the messaging industry do not apply to two-way voice telephony. For example, traditional paging providers and SMR providers can meet the assistance capability requirements by providing cloned subscriber units. Cloning, however, has no applicability to wireline or wireless telephony. Thus, the Commission cannot operate under a “one standard fits all technologies” paradigm in interpreting CALEA.

Further, if the Commission were to apply the J-STD-025 to other industries by mandating the provision of features such as packet data and location information, it would be contravening Section 107(a)(2), which permits industry associations or standards-setting organizations to develop safe harbor standards.⁹⁶ As discussed above, the paging industry, for example, has already promulgated safe harbor standards for Traditional Paging and Advanced Messaging. These standards, as envisioned by Congress in drafting Section 107(a)(2), were developed by industry members based on the legal requirements of CALEA, and the technical capabilities of messaging systems. It would defy the intent of Congress to impose a standard developed for

⁹⁶ 47 U.S.C. § 1006(a)(2).

wireline and broadband CMRS carriers on other industry segments without their input or consent.

Ultimately, if “a Government agency or any other person” believes an industry-promulgated standard to be deficient, it must challenge the standard by filing a petition for rulemaking with the FCC.⁹⁷ Thus, if any party wishes to see particular feature that has been included in J-STD-025 incorporated into the technical standard governing another communication service or services, that party must either take part in the standards setting process or file a petition for rulemaking with the FCC after a standard has been set. It is not, however, consistent with CALEA to superimpose one industry segment’s standard on another industry segment.⁹⁸

VIII. CONCLUSION

Consistent with the statutory definition of the assistance capability requirements, J-STD-025 represents a delicate compromise between the needs of law enforcement officials, the technical capabilities of the telecommunications network, and implementation costs.

⁹⁷ 47 U.S.C. § 1006(b).

⁹⁸ Much more troubling to members of the wireless industry is the lack of any statute of limitations for bringing a deficiency challenge. This apparent oversight by the Congress makes CALEA compliance an even more burdensome prospect than most parties appreciate.

The Commission should therefore sanction J-STD-025 as the technical standard for two-way voice telephony without adding any of the punch list items. Such Commission action will lead to the implementation of a standard that meets the legitimate needs of law enforcement officials without forcing unnecessary costs on the American public.

Respectfully submitted,

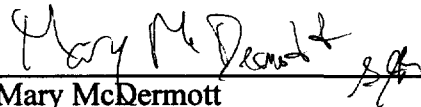
PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION

By:



Eric W. DeSilva
Stephen J. Rosen
Daniel J. Smith
WILEY, REIN & FIELDING
1776 K Street, N.W.
Washington, DC 20006-2304
(202) 429-7000

By:



Mary McDermott
Senior Vice President/Chief of Staff for
Government Relations
Todd B. Lantor
Manager, Government Relations
PERSONAL COMMUNICATIONS
INDUSTRY ASSOCIATION
500 Montgomery Street, Suite 700
Alexandria, VA 22314
(703) 739-0300

Its Attorneys

December 14, 1998